暗号ハードウェアのセキュリティ

Ph.D. 崎山　一男
博士（情報科学） 菅原　健 共著
博士（工学） 李　陽

コロナ社

ま　え　が　き

情報通信ネットワークのオープン化が進む中で，ネットワークセキュリティ，システムセキュリティの確保が最重要課題となっている。情報漏えい対策に対する社会の強いニーズに鑑み，本書で取り扱う内容として，情報・制御システムを含む社会インフラの安全・安心を支えるハードウェアのセキュリティ技術（hardware security）を基礎から解説する。暗号ハードウェア（cryptographic hardware）の物理攻撃（physical attack）や安全性解析を中心に，セキュリティエンジニアに必要となる知識を理論から実践まで網羅する。

スマートフォン（smartphone）やネットワーク家電など，あらゆる情報機器がネットワークに接続され，クラウドサーバ（cloud server）を中心としたさまざまなサービスが展開されている。この結果，新たなビジネス分野が創出され，日常生活における利便性が向上している。

一方で，ネットワーク上に流れる情報漏えいが社会問題となっている。この種の問題のほとんどが，人為的なミスに起因するといっても過言ではない。したがって，情報セキュリティ確保の第一歩は，情報システムを設計・開発・運用する高度技術者が，適切に情報リテラシー（literacy）を身につけることである。設計・開発者は，情報は漏えいするものという観点から，システムの脆弱な部分を見つけ，その部分の強化を図らねばならない。意図的に情報を盗み取ろうとする攻撃者は，システムの最も脆弱な部分（weakest link）を狙ってくるからである。

暗号技術は，情報セキュリティの基盤技術の一つとして経済活動や社会生活に広く浸透してきた。暗号技術が提供する秘匿通信（secure communication）や利用者の認証（authentication）やサービスの真正性（authencity）の保証などは，情報セキュリティを達成するのに欠かせないものである。具体的な応

用例としては，暗号電子メールや電子商取引に用いられる SSL（secure socket layer）/TLS（transport layer security），利用者認証や電子マネーに用いられる SIM（subscriber identity module）カード，パーソナルコンピュータ（personal computer，PC）の個体識別やデータの保護などを提供する TPM（trusted platform module），マイクロプロセッサ（microprocessor）にセキュアな領域を確保する TEE（trusted execution environment）などが挙げられる。

情報システムへの暗号技術の導入により，多くのセキュリティ上の問題が回避できていることはいうまでもない。しかしながら，暗号技術を実装した際に生じる新たな問題にも直面している。暗号技術の理論的観点における想定と，物理的観点における現実との間のギャップを巧妙につく，いわゆるサイドチャネル攻撃（side–channel attack）を代表とする物理攻撃の脅威である。

本書の目的は，暗号ハードウェアの安全性に関する基礎知識を身につけることである。学部生，大学院生，セキュリティエンジニア/研究者を対象として，学術的に重要と思われる基礎的な攻撃手法や対策技術を厳選している。本書を読むにあたって，計算機アーキテクチャ，暗号理論，および数論アルゴリズムの基礎知識を前提としている。高度な攻撃が続々と登場する中，情報を守る最後の砦であり，信頼の基点（root of trust）である暗号ハードウェアの重要性は増すばかりである。その基礎を学ぶ本書が，安心・安全な情報社会の一助となれば幸いである。

本書出版にあたっては，多くの方からご協力をいただいた。まず，電気通信大学の授業「ハードウェアセキュリティ」のティーチングアシスタントを担当してくれた中曽根 俊貴さん，松原 有沙さん，町田 卓謙さん，粕谷 桃伽さん，庄司 奈津さんからのフィードバックは非常に役に立った。辰巳 恵里奈さん，羽田野 凌太さんには本書で扱うデータや図の作成に協力いただいた。この場を借りて感謝したい。また，本書出版の労をとってくださったコロナ社に厚くお礼申し上げる。

2019 年 5 月

崎山　一男

目　　次

1. 暗号技術と暗号ハードウェアへの脅威

2. 共通鍵暗号の実装

3. 公開鍵暗号の実装

4.　暗号モジュールへの脅威と対策

5.　サイドチャネル攻撃

6. フォールト攻撃

7. マイクロアーキテクチャへのサイドチャネル攻撃

1 暗号技術と暗号ハードウェアへの脅威

1.1 はじめに

高度に発達した情報化社会により，私たちの生活は劇的に変わった。多種多用なデータがデジタル情報に変換され，オープンネットワークであるインターネット上に流れるようになった。デジタル情報保護の必要性から，現代の暗号技術は急速に普及し，個人情報の**漏えい**（leakage），他人への**なりすまし**（impersonation），データの**改ざん**（manipulation）といったセキュリティ上の多くの問題を未然に防ぐことに貢献している。

現在，広く利用されている**暗号**（cryptography）技術は，比較的新しい技術である。その基礎となる学術研究が活発となったのは，1970 年代以降である。また，マイクロプロセッサ上のソフトウェアや専用のハードウェアで暗号処理が実装できるようになり，民生品などの分野で暗号技術が普及したのは，1980 年代に入ってからである。AES 暗号として広く知られている，ブロック暗号（2.1.3 項 参照）**ラインダール**（Rijndael）が登場したのは，1990 年代の後半である。

最近では，暗号処理に必要なハードウェア一式をモジュール化し，暗号モジュールとして製品化されることが多い。モジュール実装の形態をとることで，各部品の入出力部にプローブを当てて盗聴を試みるプロービング攻撃（4.1 節 参照）や，ROM の内容を暴くリバースエンジニアリング（reverse engineering）を困難にしている。さらに，モジュール内の暗号アルゴリズムを処理するハード

ウェアについては，通常，暗号専用の処理回路が用いられ，限られた計算資源（computational resource）で，あらゆる現実の攻撃に耐えうる安全性と，暗号処理によるオーバーヘッドを低減する高速処理を実現している。代表的な暗号モジュールは，**スマートカード**（smartcard）である。スマートカードは，マイクロプロセッサ，ROM，RAM，暗号専用の処理回路といった部品を 1 チップで実現し，プラスチックカード上に搭載したものである。**RFID**（radio frequency identification）**タグ**や**センサノード**（sensor node）といった，さらに計算資源の乏しいデバイスへの暗号技術の導入が期待されており，暗号モジュールの需要はますます高まるものと考えられる。

理論上，攻撃者は，暗号アルゴリズムにおける中間値を知ることはできない。これは，暗号モジュールが，完全なブラックボックスとして機能することを意味する。しかし，実際の暗号モジュールは，完全なブラックボックスではない。攻撃者は，暗号モジュール実装の不備を突き，物理的にアクセスして攻撃を仕掛けるのである。このように，安全な暗号システムを実現するためには，理論上の安全性だけでなく，実装上の安全性をつねに意識しなければならない。

1.2　暗号技術の概要

情報セキュリティ（information security）技術の目的は，これらの脅威に対し，以下に示す三つの性質を実現することで安全性を保証することにある。

- **秘匿性・機密性**（confidentiality）：　権限のない第三者から情報の内容が隠されていること
- **完全性・整合性・一貫性**（integrity）：　情報が正真であり，改ざんされていないこと
- **可用性**（availability）：　権限がある者はいつでも情報が利用できること

多様化する情報システムにおいて，どのような攻撃から，どのような情報を守りたいのかというセキュリティ要求は，システムごとにさまざまである。要求によって，実装されるセキュリティプロトコルは異なり，必要とされる基本

的な構成要素である**ビルディングブロック**（building block）も異なる。多くのプロトコルで共通に用いられるビルディングブロックは，公開鍵暗号（PKC），共通鍵暗号，暗号学的ハッシュ関数，および乱数生成器（RNG）である。最近では，物理的固有性を暗号鍵の生成や認証に利用する**複製困難関数**（physical unclonable function，**PUF**）も新たなビルディングブロックとして期待されている。こういった基本的な暗号演算を，**暗号プリミティブ**（cryptographic primitive）と呼ぶ。

1.3 ハードウェア実装される代表的な暗号プリミティブ

1.3.1 公開鍵暗号

公開鍵暗号（public–key cryptography，**PKC**，3 章 参照）**方式**では，**暗号化鍵**（encryption key）と**復号鍵**（decryption key）は異なる。事前に鍵を共有することなく，秘匿通信を実現できる点が特徴的である。インターネットのように，鍵を安全に配送することが困難なシステムにおいては，必須の技術である。

暗号アルゴリズムとしては，RSA 暗号と楕円曲線暗号（ECC）が有名である。共通鍵暗号方式では，計算機で容易に処理できる演算を組み合わせることで，少ない計算資源で構成できるように工夫されているが，公開鍵暗号ではそのような工夫が難しい。それは，公開鍵暗号の演算において，例えば 2 048 ビットの剰余乗算といった多倍長整数に対する演算を繰り返し実行する必要があるからである。そのため，共通鍵暗号と比べてより多くの計算資源を必要とする。実装に関する詳細は，3 章で説明する。

1.3.2 共通鍵暗号

共通鍵暗号（symmetric–key cryptography，2 章 参照）**方式**では，暗号化と復号に同じ鍵を用いる。処理が高速であることが最大の利点であり，ワイヤレスルータ向けの高スループットな暗号化や交通系 IC カードに求められる低

レイテンシーな認証に適している†。ただし，共通鍵暗号方式を実現するためには，送信者と受信者は事前に鍵を共有しておく必要があり，システムによっては鍵の配送や管理が困難となる場合がある。

共通鍵暗号方式は，計算が容易な変換処理を繰り返し適用することで，ソフトウェアやハードウェアにおける高速実装を可能としている。共通鍵暗号として，メッセージを一定の長さのブロック単位ごとに切り出して処理を行うブロック暗号（2.1.3 項 参照）と，ビット単位あるいはバイト単位ごとに処理する**ストリーム暗号**がある。現在，最もよく使われているブロック暗号である AES 暗号については，2 章で詳しく紹介する。

1.3.3　暗号学的ハッシュ関数

暗号学的ハッシュ関数（cryptographic hash function）は，任意長のメッセージから，一定の長さの値（ハッシュ値）を算出するアルゴリズムである。どんな入力メッセージに対しても，ハッシュ値を求めることは容易であるが，所望のハッシュ値となるようなメッセージを見つけることは困難となるように設計される。ハッシュ関数の出力値は，メッセージ全体を要約して得られた代表値であるため，**メッセージダイジェスト**（message digest）とも呼ばれる。

ハッシュ関数は，主にデータの完全性検証に用いられる。例えば，アリスがボブにメッセージを送る際に，送付したメッセージが正しいものかをボブが知りたいとする。このとき，アリスはメッセージ m から，ハッシュ値 $D = H(m)$ を計算し，m と D の両方をボブへ送付する。ボブは，受け取ったメッセージ m からハッシュ値を再計算し，アリスが送ってきたハッシュ値 D と一致するかを検証する。マロリーは，m と同じハッシュ値をもつ異なるメッセージ m' の作成を試みるが，ハッシュ関数の性質により非常に困難である。したがって，ハッシュ値の不一致が確認された場合には，能動的攻撃者マロリーにより m が改ざんされたことを検知できる。

† スループットとは単位時間当りの処理データ数を指し，レイテンシーは入力データの処理が終わるまでの時間を指す。

暗号学的ハッシュ関数の特徴として，以下の三つの性質は必須である。

- **原像困難性**（preimage resistance）： ハッシュ値 $H(m)$ が与えられたとき，対応するメッセージ m を見つけることが困難であること
- **第二原像困難性**（second preimage resistance）： メッセージ m_1 が与えられたとき，$H(m_1) = H(m_2)$ を満たす m_2（$\neq m_1$）となるメッセージ m_2 を見つけることが困難であること
- **衝突困難性**（collision resistance）： ハッシュ値が一致するような異なる二つのメッセージを見つけることが困難であること

1.3.4 乱数生成器

通信路を盗聴する攻撃者が使う攻撃手段の一つは，過去に盗聴・録音したメッセージを再送することである。そのような攻撃をリプレイ攻撃（replay attack）と呼ぶ。リプレイ攻撃を防ぐには，通信路を流れるデータが毎回異なっていなくてはならない。そのような目的のために，暗号では乱数が多用される。乱数を発生するハードウェアやソフトウェアを**乱数生成器**（random number generator，**RNG**）と呼ぶ。

シミュレーションなどで用いられる乱数生成アルゴリズム（例えば C 言語の `rand` 関数）は，攻撃者が乱数を予想できてしまうため，暗号に用いることはできない。暗号のための乱数は，過去の乱数を見ても将来の乱数を推測できない，という性質を備える必要がある。そのような乱数を「暗号学的に安全な乱数」と呼ぶ。

熱雑音や量子現象などの自然現象から乱数を取り出すためのハードウェアを**真性乱数生成器**（true random number generator，**TRNG**）と呼ぶ。また，与えられた初期値（**シード**，seed）から暗号学的に安全な乱数の系列を生成するためのアルゴリズムを**疑似乱数生成器** (pseudo random number generator，**PRNG**）と呼ぶ。低速な TRNG で生成した乱数を，高速な PRNG のシードとして利用するという方法が一般的である。

索　　引

——著 者 略 歴——

崎山　一男（さきやま　かずお）
1994年　大阪大学基礎工学部電気工学科卒業
1996年　大阪大学大学院修士課程修了（物理系電気工学分野）
1996年　株式会社日立製作所
2003年　カリフォルニア大学ロサンゼルス校 M.Sc.コース修了（EE 専攻）
2007年　ルーヴェン・カトリック大学 Ph.D.コース修了（ESAT/COSIC 専攻）
　　Ph.D.
2008年　ルーヴェン・カトリック大学ポスドク研究員
2008年　電気通信大学准教授
2013年　電気通信大学教授
　　現在に至る

菅原　健（すがわら　たけし）
2006年　東北大学工学部情報工学科卒業
2008年　東北大学大学院博士前期課程修了
　　（情報基礎科学専攻）
2010年　Cryptography Research Inc. イン
　　ターン
2011年　東北大学大学院博士後期課程修了
　　（情報基礎科学専攻）
　　博士（情報科学）
2011年　三菱電機株式会社情報技術総合研究所
　　研究員，主席研究員
2017年　電気通信大学准教授
　　現在に至る

李　陽（り　やん）
2008年　ハルビン工程大学水声工程学部
　　電子情報工程学科卒業
2011年　電気通信大学大学院博士前期課程修了
　　（情報通信工学専攻）
2012年　電気通信大学大学院博士後期課程修了
　　（総合情報学専攻）
　　博士（工学）
2013年　電気通信大学産学官連携研究員
2013年　電気通信大学特任助教
2015年　南京航空航天大学准教授
2018年　電気通信大学准教授
　　現在に至る

暗号ハードウェアのセキュリティ

Cryptographic Hardware Security

2019 年 6 月 13 日　初版第 1 刷発行　★

検印省略

著　者　崎山　一男
　　菅原　健
　　李　陽
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　三美印刷株式会社
製本所　有限会社　愛千製本所

112–0011　東京都文京区千石 4–46–10
発行所　株式会社　コロナ社
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140–8–14844・電話(03)3941–3131(代)
ホームページ　http://www.coronasha.co.jp

ISBN 978–4–339–02894–2　C3055　Printed in Japan　（金）